key on. Alternatively, Combination keys can be used to allow LDs to be authenticated individually. This may sometimes be useful for management operations. The disadvantage is that a separate Link key has to be stored on the KD for each LD.

Changing the Unit key of a KD will make all locks fail authentication to the KD. However, the KD will still be authenticated to the locks since the KD's RSA pair is used for that. Thus, the KD will still be able to open LDs.

LIDs are hierarchical(e.g. "customer number" - "site number" - "lock number") to facilitate master keys. If a KD can open an LD, it can also open any LD beneath it in the hierarchy. Technically this is only necessary for the tickets, since the KDs rely on the LDs to check whether their public key is stored on the LD or not.

Finally, note that the wireless nature of the solution allows LDs to be placed inside the door, making tampering impossible. If the LD includes an emergency power socket for out-of-power KDs, the socket has to be located on the outside, but since it is used solely for power transfer it cannot be used for tampering with the lock. Of course, placing the LD on the inside of a door is feasible only if there is some other way of getting inside if the LD malfunctions.

KDs and LDs are controlled via separate control device (hereafter CD), that also includes a Bluetooth device. LDs can also have a built-in CD, or a wireline connection to an external control system.

A CD is also a KD. The access rights for the CDs public key stored on the lock must enable control operations.

To create initial keys, an LD PIN is used (as per Bluetooth specification) for both authentication and encryption. The KD PIN is used for authentication and encryption between KDs and CDs.

If the Bluetooth technology is successful, many mobile phones will be equipped with Bluetooth devices to enable them to be connected to similarly equipped computers. A Bluetooth-enabled mobile phone is also an optimal CD:

- Most people will have one.
  - PIN-based KD security controls (e.g. enable/disable KD) can be tied to those of the phone (e.g. enable/disable outgoing calls).
  - Keys and tickets can be transmitted with the phone.
  - A phone can also itself function as a KD. This is extremely valuable, since it would make achieving "critical mass" for the system much easier.

A key can be created whenever the LD and the KD are in contact. A CD must be used to activate the LDs key creation sequence. The LD will then show (via the controller) the user names of all unknown key devices in range. A key device is selected by the user of the LD.

Optionally, a temporary PIN code can be selected for authentication and encryption between the LD and the KD, as per Bluetooth specification. In that case, the PIN must also be entered to the KD using a controller.

The LD sends a key registration request to the KD. If a temporary PIN was not used, the KD signals the user of the KD via the confirmation request output device, and awaits an action on the confirmation input device. After the used has activated the input device, the KD sends its KID, user name, link key and public key to the LD. Access rights for the KD must then be entered to the LD via its CD.

The link key is either the KD's Unit key, or a combined key can be created (as per Bluetooth specification). In the latter case, both the combined key and the LID must be

stored on the KD. In any case, the KD may store the LID to keep track of the locks it has access to.

KD registration can be done remotely by sending the above information via any electronic media to the controller. While the media need not be secure against eavesdropping, it should be secure against an attacker replacing the information with his own.

A KD that is not a CD can also have the right to create new keys. In that case, a CD must be used to ask the KD to create the key and for controlling the process. The KD will effectively act as a mediator between the CD and the LD.

Turning now to the drawings, the method of operation of these devices is now described. The numbering in the flowcharts follows the following conventions:

- The first digit in a number is the number of the figure. Thus, when a number is given, a reference to the figure is not necessary.
- Even thousands signify the whole flowchart, and are only used in flowchart references (e.g.5000 signifies the flowchart in Fig. 5).
- Except for iteration and flowchart references, the numbering is ordered so that if item X happens after item Y, then X has a number greater than Y.

Figure I shows an embodiment of the process of using a key, from the KD point of view, as a flowchart. Figure 2 shows an embodiment the process of using a key, from the LD point of view, as a flowchart.

1) The LD broadcasts its service (2020, 1020).
2) The KD sends its KID (1030, 2030) to the LD, which looks up the KID in its database (2040). The LD then replies with its LID, Confirm flag and a flag that tells if the lock knows the KID (true in this case) (2050, 1040). If the confirm flag was